UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/468,747	12/21/1999	XIN WANG	D/99164Q	4043

7590 09/12/2003

Marc S. Kaufman
NIXON PEABODY LLP
8180 Greensboro Drive
McLean, VA 22102

EXAMINER	
KIM, JUNG W	
ART UNIT	PAPER NUMBER
2132	10

DATE MAILED: 09/12/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/468,747	**Applicant(s)** WANG, XIN	
	Examiner Jung W Kim	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-7 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-7 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 December 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 6,7,8,9 .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement filed on December 21, 1999 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each U.S. and foreign patent; each publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. Several foreign patent documents and a non-patent document were not submitted and have not been considered by the office (see IDS on paper #9).

Specification

2. The disclosure is objected to because of the following informalities: on page 6, line 9, the phrase "the schemes themselves do not help specifying who is the key holder" should read "the schemes themselves do not help specify who is the key holder"; on page 6, line 14, the phrase "One very appearing feature" should read "One very appealing feature"; on page 6, line 22, the sentence is not grammatical; on page 7, line 2, the sentence is not grammatical; on page 9, line 5, the indefinite article 'an' should be 'a'; on page 20, line 16, there is an extraneous indefinite article; on page 23, line 5, the sentence is not grammatical; on page 43, line 21-22, the sentence is not grammatical. Appropriate correction is required.

3. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-4 are rejected under 35 U.S.C. 102(b) as being anticipated by Schneier Applied Cryptography 2nd Edition (hereinafter Schneier). As per claim 1, Schneier teaches a method for protecting a data file on a computer system, comprising the following steps:

a) encrypting the data file using a key to create an encrypted data file (see Schneier, page 4, 'Symmetric and Public-Key Algorithms'; page 179-180, 'Using Keys');

b) generating a new key (see Schneier, page 180, 'Updating Keys');

c) updating the encrypted data file with the new key to create an updated encrypted data file and replacing the encrypted data file with the updated encrypted data file. Schneier teaches that keys must be replaced regularly and that old keys must be destroyed (see Schneier, page 183, 'Lifetime of Keys', page 184, 'Destroying Keys'). Furthermore, Schneier teaches a focal point of encryption: encryption is to make files unrecoverable without the key (see Schneier, page 181, 'Backup Keys'). Hence, the update and replacement steps are necessary to maintain consistency within the system disclosed by Schneier;

d) replacing the key with the new key (see Schneier, page 180, 'Updating Keys'; page 182, 'Compromised Keys'; page 183, 'Lifetime of Keys'; page 184, 'Destroying Keys').

The aforementioned covers all of claim 1.

6. As per claim 2, Schneier covers a method for protecting a data file on a computer system as outlined above in the claim 1 rejection under 35 U.S.C. 102(b). In addition, as mentioned above, Schneier teaches that keys must be replaced regularly (see Schneier, page 183, 'Lifetime of Keys'; page 184, 'Destroying Keys'). As such, Schneier covers the step of repeating the updating step and the two replacing steps on a periodic basis.

7. As per claim 3, Schneier covers a method for protecting a data file on a computer system as outlined above in the claim 1 rejection under 35 U.S.C. 102(b). In addition, inherent in the steps to replacing the encryption key and updating the encrypted document, is the step of replacing the decryption key [this step is operatively identical to replacing the encryption key for those systems utilizing symmetric keys]. The replacement of the decryption key is a necessary step to maintain consistency within the system disclosed by Schneier.

8. As per claim 4, it is an apparatus claim corresponding to claims 1-3 and it does not teach or define above the information claimed in claims 1-3. Therefore, claim 4 is rejected as being anticipated by Schneier for the same reasons set forth in the rejections of claims 1-3.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 5-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Lewis U.S. Patent No. 5,761,306 (hereinafter Lewis). As per claims 5-7, Schneier covers an apparatus to protect a data file outlined above in the claim 4 rejection under 35 U.S.C. 102(b). Schneier does not teach a smart card comprising a processor and memory having functions as outlined in claim 4 by the applicant. However, Lewis discloses a smart card that is implemented in a processor-driven system. In the invention disclosed by Lewis, a smart card includes a processor for protecting personal data and a memory coupled to the processor for storing personal data (see Lewis, col. 11 line 64-col. 12, line 6; Figure 3 and related text). Also disclosed by Lewis is a key server to create new keys for the smart card when the existing key stored on the smart card needs to be replaced (col. 10, lines 30-58; Figure 3 and related text). Finally, the processor-driven system disclosed by Lewis comprises a

communication interface (see Lewis, Figure 3 and related text). It would be obvious to one of ordinary skill in the art at the time the invention was made to implement a processor and memory with functions as outlined in claim 4 by the applicant, into a smart card as disclosed by Lewis. The motivation for such a combination would be to ensure the security of data stored on a smart card in the case when a key used for encryption by the card is compromised.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Jakobsson U.S. Patent No. 6,587,946 discloses a method and system for controlled asymmetric proxy encryption.

Chan et al. U.S. Patent No. 6,005,942 discloses a system and method for a multi-application smart card.

Misra et al. U.S. Patent No. 6,189,146 discloses a system and method for software licensing.

Spelman et al. U.S. Patent No. 5,680,458 discloses a root key compromise recovery system.

Cooper et al. U.S. Patent No. 5,563,946 discloses a method and apparatus for enabling trial period use of software products.

Bruwer U.S. Patent No. 6,191,701 discloses a secure self learning system.

Seheidt et al. U.S. Patent No. 5,375,169 discloses a cryptographic key management method and apparatus.

Chandra et al. U.S. Patent No. 4,817,140 discloses a software protection system.

Arnold et al. U.S. Patent No. 4,558,176 discloses a computer system to inhibit unauthorized copying or usage, and automated cracking of protected software.

Atalla UK Patent Application GB2136175A discloses a file access security method and means.

Sakakibara et al. 'The ID-based Non-interactive Group Communication Key Sharing Scheme using Smart Cards' discoses a group communication key sharing scheme based on a modified copy key method using n-pieces of a key for n members of the group.

Abadi et al. 'Authentication and Delegation with Smart-cards' discloses several principles in the course of authentication in smart-card protocols.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00 A.M. to 5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Jung W Kim
Examiner
Art Unit 2132

Jk
September 2, 2003

Gilberto B

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100